

Amendments to the Claims

1. (Currently amended) A system for network security comprising:
 - a first network device having a first set of key material ~~with a first base key and a key extension~~, the first set of key material including a first base key and a key extension in addition to the first base key;
 - a second network device having the first set of key material and a second set of key material ~~with a second base key~~, the second key material including a second base key, wherein the second network device ~~being~~ is capable of communicating with the first network device using security determined by the first set of key material; and
 - a third network device having the second set of key material, wherein the third network device ~~being~~ is capable of communicating with the second network device using security determined by the second set of key material[;] , and

wherein the security determined by the first key material is stronger than the security determined by the second set of key material.
2. (Original) The system of claim 1 wherein the first base key and the key extension together form a first encryption key, the first encryption key being used to encrypt communications between the first and second network devices, and the second base key forms a second encryption key, the second encryption key being used to encrypt communications between the second and third network devices.

3. (Original) The system of claim 2 wherein the first encryption key has a length of greater than a threshold number of bits, and the second encryption key has a length of no greater than the threshold number of bits.

4. (Original) The system of claim 3 wherein the threshold is 64 bits.

5. (Original) The system of claim 1 wherein the first base key and the key extension together form a first authentication key, the first authentication key being used to negotiate a first encryption key to encrypt communications between the first and second network devices, and the second base key forms a second authentication key, the second authentication key being used to negotiate a second encryption key to encrypt communications between the second and third network devices.

6. (Original) The system of claim 5 wherein the first encryption key has a length of greater than a threshold number of bits, and the second encryption key has a length of no greater than a threshold number of bits.

7. (Original) The system of claim 6 wherein the threshold is 64 bits.

8. (Original) The system of claim 1 wherein the first network device is located in a first jurisdiction, and the second network device is located in a second jurisdiction outside of the first jurisdiction.

9. (Original) The system of claim 1 wherein the first and second base keys are each based on at least a pre-shared key and a computed private key.

10. (Original) The system of claim 9 wherein the computed private key is a Diffie-Hellman key.

11. (Original) The system of claim 1 wherein the key extension is based on a hash function of an internal key and a network device identifier.

12. (Original) The system of claim 11 wherein the network device identifier is a software serial number.

13. (Currently amended) A system for network security comprising:
a first network device having a first set of key material ~~with a first base key and a first key extension~~, the first set of key material including a first base key and a first key extension in addition to the first base key, and a second set of key material ~~with a second base key and a second key extension~~, the second key material including a second base key and a second key extension in addition to the second base key;

a second network device having the first set of key material and a third set of key material ~~with a third base key~~, the third set of key material including a third base key, wherein the second network device ~~being~~ is capable of communicating with the first network device using security determined by the first set of key material; and

a third network device having the second set of key material and the third set of key

material, the third network device being capable of communicating with the first network device using security determined by the second set of key material, and the third network device also being capable of communicating with the second network device using security determined by the third set of key material [[:]] ,

wherein the security determined by the first set of key material is stronger than the security determined by the third set of key material, and

wherein the security determined by the second set of key material is stronger than security determined by the third set of key material.

14. (Original) The system of claim 13 wherein the first base key and the first key extension together form a first encryption key, the first encryption key being used to encrypt communications between the first and second network devices, the second base key and the second key extension together form a second encryption key, the second encryption key being used to encrypt communications between the first and third network devices, and the third base key forms a third encryption key, the third encryption key being used to encrypt communication between the second and third network devices.

15. (Original) The system of claim 14 wherein the first and second encryption keys each have a length of greater than a threshold number of bits, and the third encryption key has a length of no greater than the threshold number of bits.

16. (Original) The system of claim 15 wherein the threshold is 64 bits.

17. (Original) The system of claim 13 wherein the first base key and the first key extension together form a first authentication key, the first authentication key being used to negotiate a first encryption key to encrypt communications between the first and second network devices, the second base key and the second key extension together form a second authentication key, the second authentication key being used to negotiate a second encryption key to encrypt communications between the first and third network devices, and the third base key forms a third authentication key, the third authentication key being used to negotiate a third encryption key to encrypt communications between the second and third network devices.

18. (Original) The system of claim 17 wherein the first and second encryption keys each have a length of greater than a threshold number of bits, and the third encryption key has a length of no greater than a threshold number of bits.

19. (Original) The system of claim 18 wherein the threshold is 64 bits.

20. (Original) The system of claim 13 wherein the first network device is located in a first jurisdiction, and the second network device is located in a second jurisdiction outside of the first jurisdiction.

21. (Original) The system of claim 13 wherein the first, second, and third base keys are each based on at least a pre-shared key and a computed private key.

22. (Original) The system of claim 21 wherein the computed private key is a Diffie-Hellman key.

23. (Original) The system of claim 13 wherein each of the first and second key extensions is based on a hash function of an internal key and a network device identifier.

24. (Original) The system of claim 23 wherein the network device identifier is a software serial number.

25. (Currently amended) A method for network security comprising the steps of:
providing a first network device, a second network device, and a third network device;
establishing a first secure communication between the first and second network devices based on a first encryption key ~~with a base key and a key extension~~, the first encryption key having a base key and a key extension in addition to the base key;

establishing a second secure communication between the second and third network devices based on a second encryption key; and

using a stronger security for the first secure communication than the second secure communication,

wherein using the stronger security for the first communication than the second secure communication comprises using security determined by the first encryption key for the first communication and using security determined by the second encryption key for the second secure communication, and

wherein the security determined by the first encryption key is stronger than the security

determined by the second encryption key.

26. (Currently amended) The method of claim ~~[[21]]~~ 25 wherein the second encryption key is identical to the base key.

27. (Currently amended) The method of claim ~~[[21]]~~ 25 further comprising the steps of using a length of greater than a threshold number of bits for the first encryption key, and using a length of no greater than the threshold number of bits for the second encryption key.

28. (Currently amended) The method of claim 27 wherein the threshold is 64 bits.

29. (Currently amended) The method of claim ~~[[21]]~~ 25 further comprising the steps of basing each of the base key and the second encryption key on at least a pre-shared key and a computed private key, and basing the key extension on a hash function of an internal key and a network device identifier.

30. (Currently amended) A computer readable medium having stored therein instructions for causing at least one central processing unit to execute the method of claim ~~[[21]]~~ 25.

31. (Currently amended) A method for network security comprising the steps of:
providing a first network device, a second network device, and a third network device;
negotiating a first secure communication between the first and second network devices

based on a first authentication key ~~with a base key and a key extension~~, the first authentication key having a base key and a key extension in addition to the base key;

negotiating a second secure communication between the second and third network devices based on a second authentication key; and

using a stronger security for the first secure communication than the second secure communication,

wherein using the stronger security for the first secure communication than the second secure communication comprises using security determined from the negotiation based on the first authentication key for the first secure communication and using security determined from the negotiation based on the second authentication key for the second secure communication, and

wherein the security determined from the negotiation based on the first authentication key is stronger than the security determined from the negotiation based on the second authentication key.

32. (Original) The method of claim 31 wherein the second authentication key is identical to the base key.

33. (Original) The method of claim 31 further comprising the steps of deriving a first encryption key from the negotiation of the first secure communication, using a length of greater than a threshold number of bits for the first encryption key, deriving a second encryption key from the negotiation of the second secure communication, and using a length of no greater than the threshold number of bits for the second encryption key.

34. (Original) The method of claim 33 wherein the threshold is 64 bits.

35. (Original) The method of claim 31 further comprising the steps of basing each of the base key and the second authentication key on at least a pre-shared key and a computed private key, and basing the key extension on a hash function of an internal key and a network device identifier.

36. (Original) A computer readable medium having stored therein instructions for causing at least one central processing unit to execute the method of claim 31.